Information & Security

O. Polischuk
vol. 45 (2020): 7-19
https://doi.org/10.11610/isij.4501

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Ecosystem Platform for the Defence and Security Sector of Ukraine

Oleksandr Polischuk

National Institute for Strategic Studies, Kyiv, Ukraine
https://niss.gov.ua/en

ABSTRACT:

While success in current and future conflicts will increasingly be predicated by optimisation of high-tech solutions rather than military capabilities based on mass, the application of modern business approaches is of key importance for reforms aiming to adapt security and defence to the new realities. This article presents detailed analysis of ways to adapt the security and defence sector of Ukraine to Euro-Atlantic standards, taking into account Ukraine's trajectory and growing interaction with the international security systems and the specific context shaped by the external aggression against Ukraine. Based on the analysis of existing legislation and review of theoretical sources, the author concludes that the present archaic, post-Soviet type security and defence sector of Ukraine is not adequate to the future complex challenges. Further, he applies the ecosystem approach to elaborate recommendations for the development of a modern model of national security and defence organisation based on functional integration of the capabilities of all main security and defence actors, emphasising the strategic importance of the integration of Ukraine's security and defence sector into European and Euro-Atlantic security systems.

ARTICLE INFO:

RECEIVED: 26 MAR 2020
REVISED: 06 APR 2020
ONLINE: 14 APR 2020

KEYWORDS:

security and defence sector, defence ecosystem, complex systems, hybrid war, capabilities, clusters, ecosystem approach, comprehensive approach, block chain

E-mail: olexandryt@gmail.com

Problem Formulation

The development of effective security and defence arrangements are widely studied by Ukrainian and foreign experts. For example, authors of the scientific study from the National Security Academy "The Ukrainian security and defence sector: theory, strategy, practice"[1] have identified optimal models for the national security and defence arrangements. However, their study does not touch upon the development of effective interrelationships and potential synergies between the constituent components of the system.

The first step towards strategic changes in the sphere of national security, proposed by Volodymyr Gorbulin and Anatoliy Kachyns'kyj, is the "definition of the individual contribution to national security of each component of the national security system of the state."[2] The process of creation of the Security and Defence Sector (SDS) of Ukraine as a holistic system was launched back in 2007 following the requirements of the National Security Strategy [3]; however, it was not completed due to the lack of political will and a clear vision on the division of responsibilities between the systems' components and on the integral basis for their interaction. These deficiencies were highlighted in the 2015 version of the National Security Strategy.[4] The new Strategy stressed that the SDS of Ukraine is not shaped as a holistic and unified entity, guided from a single centre; that there is an institutional weakness; lack of professionalism; structural imbalance of security and defence sector components; lack of resources and inefficient use of resources in the security and defence sector.[5]

As a result of such inadequacies, the SDS of Ukraine does not provide timely and effective response to a wide spectrum of threats, generated primarily by the aggressive policy of Russia, as clearly drawn from the results of defence reviews in Ukraine of 2014 and 2019.[6] In this respect, the main instrument of pressure on Ukraine is the combination of 'hard power' in the form of open armed aggression with 'soft power' influence focused mainly on the economic, media, and social spheres of the Ukrainian society. Here, the hybrid character of the modern war prevails over the physical one.

Attempts of the SDS components to create institutionally self-sufficient systems of reaction to the whole spectrum of threats through development of respective capabilities leads to duplication, complication of the management system and inefficient use of resources. The SDS at present has a limited capacity to respond coherently to modern threats as a result of ineffective interagency cooperation.

So far, there is no extensive research on the construction of SDS as a complex, cluster-type integrated system based on open information platforms. The implementation of such approach would allow concentration and multiplication of the necessary capabilities to perform effectively in a range of scenarios. While the main capabilities will be provided by state agencies, the concept of outsourcing certain capabilities can also be implemented.

The purpose of this study is to prepare recommendations for introducing the most effective model of national security and defence in Ukraine and thus enhance its capacity to fulfil its fundamental constitutional function – to guarantee the security for the citizens and the state.

Therefore, the first section of this article is devoted to analysis of the international best practices and current scientific achievements and reveals the major trends in the development of national defence systems. The analysis of Ukraine's existing national security system, provided in the second part of the study, detects the most problematic areas in its ability to respond to actual and potential threats. The third section focuses on the transformation of Ukraine's defence sector through implementation of best practices, changes in the strategic culture inside of system, and the adaptation of national legislation to NATO and EU policies. The conclusions and recommendations provided in the final section of the study should help decision makers to build a modern defence model of Ukraine.

Defence Ecosystems in Theory and Practice

Back in 1935, the British botanist and pioneer in the ecology science Arthur Tansley introduced the term "ecosystem."[7] It was commonly used to refer to natural living organisms that had adapted themselves to coexistence in one environment – the biotope, forming a coherent system. Each individual in such a system has its own role and own relations with other entities. The system is self-regulated by natural rules.

In the early 1960s, the Canadian philosopher Marshall McLuhan formulated the term "media ecology" and developed the media ecology theory – the study of impact of media, technology, and communication on the human environments.[8] This theory is still valid in the context of modern hybrid wars.

The term "urban ecosystems" was introduced in the 1980s.[9] Today, it is widely used, e.g. by the Australian national science agency (Commonwealth Scientific and Industrial Research Organisation) which studies cities as integrated social-ecological systems with the aim to develop sustainable approaches for urban design that reduce negative impact on surrounding environments.

Uncertainty and diversity of the modern world, the complexity of hybrid threats gave birth to a new approach for defence in the first decade of the XXI century. The Royal United Services Institute (RUSI) introduced the notion of a defence industrial ecosystem as an analytical tool for discussion on the nature of the roles of defence manufacturing and service industries in a complex world.[10]

In 2017, the British researcher Richard Fisher from Cranfield University prepared a brief guide on the networks and relationships of the entire defence ecosystem and how they operate as part of the £ 30 billion turnover across the defence and security industries.[11] The hybrid nature of modern security threats requires the involvement of organisations which have been never considered as part of defence systems, but could play a crucial role in achieving victory. In his research paper Fisher states: "Considering any industry as an ecosystem begins

to imply how simple changes in one area can permeate throughout and there is often reliance upon an area that may not be known about."

For example, the US intelligence ecosystem is built on an open communication platform in the framework of the Intelligence Advanced Research Projects Activity (IARPA) based at Maryland University. This intelligence ecosystem consists of 16 national agencies and 1271 other state bodies and 1931 commercial companies.[12]

Experts of The Hague Centre for Strategic Studies consider defence as a social technology which consist of four-tiered classification, including Netherlands Defence and Security Ecosystem of the highest level.[13]

Canada's national innovation ecosystem consists of public sector institutions, private sector businesses, and academic organizations that offer business resources and support services to Canadian companies and Armed Forces in order to meet the requirements to Canadian defence through effective collaboration.[14]

The need for more effective interagency cooperation in counter-terrorism, with a particular focus on intelligence sharing, was highlighted in the research of Iztok Prezelj and Joe Aire.[15]

Cybersecurity is probably one of the most complex areas requiring a broad spectrum of competencies, human, technological and financial resources united in a collaborative network for effective response to the growing threats. George Sharkov studied cyber resilience models and elaborated on multi-stakeholder engagement and partnership for the implementation of a national cyber resilience collaborative framework.[16] To be effective and sustainable, such collaboration is based on governance mechanisms meeting a variety of requirements. In a recent study on organisational collaboration in the field of cybersecurity, Todor Tagarev addressed comprehensively the governance requirements to networked organisations.[17]

The holistic view allows to determine some of the basic principles for building up the defence ecosystems: engaging multiple stakeholders and customers, unity of effort, collaborative network, sharing innovation, collective management of risks, civil-military collaboration, integrity of governmental and non-government organisations, cohesion and comprehensiveness. In addition, and as pointed in the Strategy for Development of the Defence Industrial Complex of Ukraine up to 2028,[18] institutional development is an internationally recognized criterion for the quality of the system's functioning, which underlines the importance of actors to interact effectively under the guidance of a single strategic management centre. In other words, institutional development should be coordinated from a single centre of competence.

The Starting Point

Ukraine's national security system is in active interaction with international security systems. That applies both to global systems, which define the strategic perspective of the state, and specific regional systems, which are in permanent

development under the influence of multi-vector powers of the global actors fighting for regional hegemony.

The effectiveness and stability of the national security system of Ukraine depend of the country's ability to react to the complex range of challenges and the need to reduce the dependencies on and the influence by external attractors. It is possible to reach such condition of the national security system by establishing a comprehensive and coordinated framework that defines aims, tasks, standards, time and resources through synchronized reform of all its agencies.

The transformation of the national security system is a complex process at the best of times, even more so given the continued military aggression against Ukraine. This unceasing aggression poses the biggest challenge to the Ukrainian state and a considerable test for its stability and resilience. Is it worth saying that reform/transformation is however essential if Ukraine is to effectively deter and counter aggression – but it should not be based merely on creation of a variation of a smaller Soviet army (Ukrainian) that fights with a larger Soviet army (that of the Russian Federation). The military should become more resilient, responsive and able to deliver asymmetric effects.

According to Paragraph 16 of Part One of Article 1 of the Law of Ukraine "On the National Security of Ukraine,"[19] the key function of the security and defence sector is defence of the national interests of Ukraine. Key components of SDS are the following:

- *Security forces* – law enforcement and intelligence bodies, state special bodies with law enforcement functions, civil protection forces and other bodies entitled by the Constitution and the laws of Ukraine to ensure the national security of Ukraine;
- *Defence forces* – Armed Forces of Ukraine, as well as other military formations, law enforcement and intelligence bodies, state special bodies with law enforcement functions created according to Ukrainian laws and entitled by the Constitution and the laws of Ukraine to ensure the defence of the state;
- *Defence industry*;
- *Citizens* and *public organisations*, which participate in ensuring the national security of Ukraine on a voluntary basis.

Hierarchic and polistructural sublevels of the SDS as well as the interdependence between its structural elements are, according to Joseph O'Connor and Ian McDermott,[20] features of a complex social dynamic system. Further, Neil Johnson, a professor at Oxford University, considers that in addition to being a collection of many interacting objects or 'agents,' a complex and effective system also contains other features. Among them are openness, communication and sharing of information, feedback between the agents, adaptability, constant interaction, emergence and absence of any sort of central controller, an intricate mix of ordered and disordered behaviour.[21]

The present SDS model exhibits only partially the features of a modern complex system; it continues to rely on hierarchic links between its actors and is

totally closed to society, thus preserving its post-Soviet nature. Internal processes in the system tend to remain poorly structured and the involvement of non-governmental actors is situational and limited. This essentially limits the capabilities of the SDS to react to the whole spectrum of threats confronting national security interests caused by the hybrid war. Moreover, the present SDS model is functioning in an inefficient manner which definitely has negative impacts on the improvement of combat capabilities of forces and decreases their operational effectiveness.

In 2018, Transparency International conducted a study of defence procurement in Ukraine in the framework of its Defence & Security Programme. The study showed that the defence sector of Ukraine obtained the lowest ranking for non-transparent procurement and high corruption risks.[22] The expenditures on defence procurement accounted for approximately 38 % (approximately 1 billion Euro) of the MoD budget. About 55 % was spent on purchases through closed procedures, and 95 % was spent on procurement of armaments and military equipment through the classified State Defence Order. According to independent expert assessments, corruption levels in these purchases was from about 5 up to 40 %.[23] In the report on the results of an audit of the effectiveness of spending budget funds allocated to the MoD for construction (purchase) of apartments for the military during 2016-2017, the state's losses estimated at approximately 66 billion Hryvna.[24] This was reflected in the report adopted on June 12, 2018 by decision # 14-1 of the Chamber of Accounts which highlighted the regular character of non-economic, non-productive and ineffective expenditures of budgetary funds during construction (purchase) of apartments, as well as the ineffective use of lands what belong to MoD and are transferred for investments in construction projects. All these facts indicate ineffectiveness in resource management and economic activities in the MoD.[25]

The Way of Transformation

According to foreign best practice, the comprehensive approach in planning and delivery of security and defence outcomes is the best means of ensuring stability. This approach should include state and non-state actors, not only national but regional and international as well.

In the framework of the Common Foreign and Security Policy of the European Union the goal of implementing a comprehensive approach was proclaimed in the European Security Strategy, adopted by the European Council on December 12, 2003. The strategy placed the emphasis on creating a "culture of coordination."[26]

At national level, the Ministry of Defence of the United Kingdom defines the comprehensive approach to the security and defence as an approach "with commonly understood principles and collaborative processes that enhance the likelihood of favourable and enduring outcomes within a particular situation."[27] The Defence Committee of the British Parliament adds that "the approach is horizontal, including both civilian and military parties and, where possible, allies and international organisations and local nationals; and vertical, taking account

of the different stages in the situation from the initial war fighting phase to reconstruction."[28]

Thus, the modern concept of the SDS envisages functional integration of capabilities of all its actors, creation of effective horizontal and vertical interrelations between them, and design and implementation of an integrated management system according to international standards. Adaptability, sustainability, self-preservation and ability to complete the tasks of the SDS system as a whole will depend on successful implementation of this concept.

Victory in present and future conflicts will belong to those who will have high-tech, adaptable and resilient armies, rather than armies based on mass. It will be not the numbers of fighting platforms to decide in the competition between defence potentials of the states, but capabilities of information systems in processing large data sets and supporting decision-making.

At present, Russia is developing its military potential by modernization of its nuclear triad as a tool of strategic superiority over the United States.[29] At the same time, in the US such an approach is considered to be an archaism of the Cold War. The Pentagon has been implementing first (nuclear weapons) and second (high precision weapons) "offset strategies."[30] Since 2015 the United States has moved towards implementation of a third offset strategy, based on the Defence Innovation Initiative – a long term program of research and design in the sphere of robotics, micro systems, artificial mind, processing of big data, 3D printing, etc. In order to protect information systems from cyber-attacks, the Pentagon plans to introduce technical decisions based on the blockchain technology.

Blockchain is based on the open network of global infrastructure and a distributed database, which is not under control of any person or company. This technology became popular in the private sector for the protection of virtual cryptocurrencies and is used in such data exchange programs as WhatsApp, Signal and Ricochet. Ukraine also plans to introduce state data management through blockchain technology.[31]

Effective security and defence sector management means the most rational use of available assets in order to react to the threats and challenges to national security in a timely and responsive manner. Present state defence programs, which define a complex of interrelated tasks and measures, directed to solve the most important national security problems,[32] almost fully reflect the principles of project management used by business corporations.

On its turn, modern businesses evolve according to the well-known since the 18th century idea of Jean-Jacques Rousseau "back to nature," which means return of society to its natural condition. This idea of the prominent French philosopher was expounded in the works of American researcher on the co-evolution in the social and economic systems James F. Moore, the inventor of the term "business ecosystem." According to Moore, such systems can also be conceived as a network of interdependent niches that in turn are occupied by organizations. Business ecosystems act according to strict rules (protocols) and play the role of "opened up" platforms for potential contributions and creative

participants.[33] As a result, this can provide a synergistic effect, which enhances the capabilities of all participants of the ecosystem, provides the opportunity to save resources and at the same time increases the value of the final product.

This concept fully reflects the strategic idea of creation of a security and defence sector of Ukraine, which is, in fact, the national security cluster. The application of an ecosystem approach in the establishment of the SDS of Ukraine addresses the problem of system integration based on the common principles for all its actors. Importantly, it provides public inclusion in the policy making process and instruments for its implementation. Moreover, its implementation will contribute to more effective use of resources and will provide opportunities for harmonised development of security and defence capabilities across all elements of the SDS and achievement of necessary levels of compatibility during the execution of joint tasks. In such a way, a comprehensive security model will be implemented and taken as a standard.

The ecosystem approach to the development of the national security system has been actively implemented since the first decade of 21st century in a number of countries such as the United Kingdom, Netherlands, Australia, New Zeeland and India.

Conclusions and Future Research

First of all, no single element of the existing national security system has the full range of required capabilities to counter modern threats. In order to respond effectively to these threats, it is necessary to develop flexible and adaptive systems that integrate the various components of the SDS.

Secondly, the value of the new model of SDS, based on numerous capacity carriers, will increase as a result of establishing effective internal interaction between them and external interaction with society. Such links should be as simple as possible to ensure synergy of effort and resources. There is also a need to give more authority and initiative to the lowest levels of government, minimizing the involvement of senior management in routine processes.

Third, the effectiveness of the whole system will depend on the balanced and coherent development of the institutional capacities of each component of the system and of the system as a whole. The national interests form the foundation for assessing the effectiveness of the security ecosystem.

Fourth, all transformation plans and programs need to be integrated into a comprehensive project portfolio that allows them to adapt and align with international initiatives. This goal can be achieved through the methodological approaches of DOTMLPFI to identify the capabilities of the security and defence sector and to consolidate them into a Single Catalogue.

Openness and transparency in the formulation and implementation of national SDS capability development plans will ensure the confidence of partners and their involvement in investment projects.

The key to security in the future and end state of national security policy should be the transition of Ukrainian society to a model of *comprehensive secu-*

rity, which includes the coordinated interaction of various actors from both governmental and non-state sectors. The implementation of the political decision related to Ukraine's goal to join the transatlantic collective security system—the North Atlantic Treaty Organization—gives all necessary practical instruments in the form of NATO standards and principles, which makes possible the development and delivery of an integrated security model.

The SDS of Ukraine must act as an opened integrated system, where the dynamics of roles played by SDS actors and their functional interaction in different security contexts will assure effective and responsive reaction to the whole spectrum of possible threats and challenges to the national security. The new SDS model is created not by the establishment of new elements, but through clear definition of their roles, responsibilities and accountabilities, and implementation of effective links between existent actors.

Amendments to Ukrainian legislation must ensure the following:

- granting the competences and authorities to the SDS actors and establishing horizontal interaction through increased coordination at the operational level;
- setting up a framework for operational integration of security sector elements through enhancement and deepening of interaction with partners in the sphere of cutting edge science, logistics, data exchange, etc., as well as elimination of technological and institutional barriers, which can compromise these processes;
- institutionalisation of multilevel interaction of the SDS actors according to the roles they play in the architecture of every separate security process, for example in the antiterrorist operation of combined and joint forces, special operations, etc.;
- creation of incentives, including fiscal incentives, in order to attract investments of the non-governmental sector into the national security dialogue.

The institutionalisation of capabilities-based planning in the SDS[34] is expected to provide opportunities to ensure a more rational and holistic basis for decision making on future defence procurement, make planning more sensitive to uncertainty, economic constraints and risks, create the basis for support to the analytical processes and make risk management easier, and promote innovation.

A group of international experts, led by Todor Tagarev, actively participated in the second defence review in Ukraine, launched in 2008. One of the recommendations to the Ukrainian government at that time was the introduction of capabilities-based planning methodology as a reliable platform for spending a limited budget in the most cost-effective way.[35] In a follow on work, Tagarev described possible degrees of cooperation and coordination within the security sector and proposed to use the capabilities-based planning as core process in security sector transformation.[36]

To harmonise the SDS ecosystem's characteristics, we can define several key development and organizational principles, which are inherent in any socio-economic system, namely: complexity, self-organization, co-evolution and adaptation.[37]

The evolution and operation of the SDS based on these principles will provide opportunities for rapid integration of national security instruments into the collective security systems, with corresponding constitutional tasks stemming from the European and Euro-Atlantic integration of Ukraine.

The effective functioning of the new national security model depends to a large extent of the establishment of effective strategic communication. The positive image of SDS entities is a key element in the formation of an attractive image of the state as a future ally in security and defence alliances.

References

1 F.V. Saganjuk, V.S Frolov, O.V. Ustymenko, M.M. Lobko, et al., *Sektor bezpeky i oborony Ukrai'ny: teorija, strategija, praktyka* [*The Ukrainian Security and Defence Sector: Theory, Strategy, Practice]* (Kiev: *Akadempres*, 2017), in Ukrainian, http://www.nationalsecurity.in.ua/sector-of-security-and-defense-of-ukraine/.

2 Vladimir P. Gorbulin, A.B., Kachyns'kyj, *Strategichne planuvannja: vyrishennja problem nacional'noi' bezpeky [Strategic Planning: Solving National Security Problems]* (Kyiv: NISD, 2010), p. 3.

3 "On the National Security Strategy of Ukraine," President's Decree #105 as of February 12, 2007, in Ukrainian, https://zakon.rada.gov.ua/laws/show/105/2007.

4 Decree of the President of Ukraine of 6 May 2015 on the Decision of National Security and Defence Council "On the National Security Strategy of Ukraine", 6 May 2015, in Ukrainian, https://zakon.rada.gov.ua/laws/show/287/2015.

5 President's Decree #287/2015 as of May 26, 2015, https://zakon.rada.gov.ua/laws/show/287/2015.

6 Strategic Defence Bulletin, "Order of President of Ukraine," № 240/2016, 6 Jun 2016, https://zakon.rada.gov.ua/laws/show/240/2016#n257.

7 See Timothy D. Schowalter, *Insect Ecology: An Ecosystem Approach*, 4th edition (London: Academic Press, 2011).

8 Robert K. Logan, "McLuhan's Philosophy of Media Ecology: An Introduction," *Philosophies* 1, no. 2 (2016): 133-140; https://doi.org/10.3390/philosophies1020133.

9 Robert B. Gibson, Donald H.M. Alexander, and Ray Tomalty, "Putting Cities in Their Place: Ecosystem-based Planning for Canadian Urban Regions," in *Eco-City Dimensions: Healthy Communities, Healthy Planet*, ed. Mark Roseland (Gabriola Island, B.C.: New Society, 1997), 25-39.

10 Henrik Heidenkamp, John Louth, and Trevor Taylor, "The Defence Industrial Ecosystem Delivering Security in an Uncertain World," Whitehall Report (London: RUSI, 2011), 2-

11, https://rusi.org/publication/whitehall-reports/defence-industrial-ecosystem-delivering-security-uncertain-world.

[11] Richard Fisher, *The Defence Ecosystem* (Cranfield, UK: Cranfield University, 2017), https://doi.org/10.13140/RG.2.2.20462.10560.

[12] Ilya Klabukov and Maksim Alekhin, "Venturnye fondy i drugie perspektivnye tehnologii dlya nacional'noi ekonomiki [The Venture Funds and Other Prospective Technologies for the National Economy]," *SSRN Electronic Journal*, 2012, p.11, https://hal.archives-ouvertes.fr/hal-01739539/document.

[13] Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs, *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-sized Force Providers* (The Hague: The Hague Centre for Strategic Studies, 2017).

[14] Thales, "Defence in Canada," 2020, https://www.thalesgroup.com/en/defence-canada.

[15] Iztok Prezelj and Joe Aire, "Interagency Cooperation in Counter-Terrorism," in *Combating Transnational Terrorism*, ed. James K. Wither and Sam Mullins (Sofia: Procon, 2016), 235-252.

[16] George Sharkov, "From Cybersecurity to Collaborative Resiliency," *SafeConfig'16: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*, Vienna, Austria, October 2016, https://dl.acm.org/doi/10.1145/2994475.2994484.

[17] Todor Tagarev, "Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives," *Future Internet* 12, no. 4 (2020), paper # 62, https://doi.org/10.3390/fi12040062.

[18] "On the Approval of the Strategy for Development of the Defence-Industrial Complex of Ukraine for the Period up to 2028, "Order of the Cabinet of Ministers of Ukraine of 20 June 2018 # 442–r, https://zakon.rada.gov.ua/laws/show/442-2018-%D1%80.

[19] Law "On the National Security of Ukraine," last amendment on March 15, 2020, https://zakon.rada.gov.ua/laws/show/2469-19.

[20] Joseph O'Connor and Ian McDermott, *Iskusstvo sistemnogo myshlenija [The Art of Systems Thinking]* (Kiev: Nika Centr, 2017), p. 36.

[21] Neil Johnson, *Two's Company, Three is Complexity* (Oxford: Oneworld Publications, 2007), pp. 13-15.

[22] Eva Anderson et al., *Six Red Flags: The Most Frequent Corruption Risks in Ukraine's Defence Procurement* (Transparency International Defence and Security and Transparency International Ukraine, September 2018), https://nako.org.ua/en/publication/six-red-flags-the-most-frequent-corruption-risks-in-ukraine-s-defence-procurement/.

[23] Anderson et al., *Six Red Flags*, p. 5.

[24] Chamber of Accounts of Ukraine, "Zvit pro rezul'taty audytu efektyvnosti vykorystannja bjudzhetnyh koshtiv, vydilenyh Ministerstvu oborony Ukrai'ny na budivnyctvo (prydbannja) zhytla dlja vijs'kovosluzhbovciv Zbrojnyh Syl Ukrai'ny, zatverdzhenyj

rishennjam vid 12.06.2018 № 14–1 [Report on the results of the audit of the effectiveness of the use of budgetary funds allocated to the Ministry of Defence of Ukraine for the construction (purchase) of housing for viscous employees of the Armed Forces of Ukraine, approved by the decision of June 12, 2018, №14-1], https://rp.gov.ua/upload-files/Activity/Collegium/2018/14-1_2018/zvit_14-1_2018.pdf.

[25] Ibid., p. 60.

[26] European Council, European Security Strategy "A Secure Europe In a Better World," Brussels, 12 December 2003, https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf.

[27] "The Comprehensive Approach," Joint Discussion Note 4/05 (London: Ministry of Defence, 2006), https://publications.parliament.uk/pa/cm200910/cmselect/cmdfence/224/22404.htm.

[28] House of Commons, Defence Committee, "The Comprehensive Approach: the point of war is not just to win but to make a better peace," Seventh Report of Session 2009–10. https://publications.parliament.uk/pa/cm200910/cmselect/cmdfence/224/224.pdf.

[29] According to the Russia's military doctrine, "Capturing the strategic initiative, preserving stable command and control of the state and the military, assuring superiority on land, sea and in air and space will become decisive factors for reaching the set objectives." *Military Doctrine of the Russian Federation*, approved by a Decree of the President of the Russian Federation, 5 February 2010, article 14 (in Russian), http://kremlin.ru/supplement/461.

[30] Robert Martinage, *Toward a New Offset Strategy Exploiting U.S. Long-term Advantages to Restore U.S. Global Power Projection Capability* (Center for Strategic and Budgetary Assessments, 2014), p. 2, https://csbaonline.org/uploads/documents/Offset-Strategy-Web.pdf.

[31] "SETAM pershymy v sviti rozpochaly vprovadzhuvaty v elektronnyh torgah tehnologiju blockchain [SETAM were the first to start to introduce the blockchain technology in the electronic bidding]," http://setam.gov.ua/article/setam-pershimi-v-sviti-rozpochali-vprovadjuvati-v-elektronnih-torgah-tehnologiyu-blockchain.

[32] Zakon Ukrai'ny "Pro derzhavni cil'ovi programy" [Law of Ukraine "On the State Special Programs"], *Vidomosti Verhovnoi' Rady Ukrai'ny (VVR)* 25 (2004): 352.

[33] James F. Moore, "Business ecosystems and the view from the firm," *The Antitrust Bulletin*: 51, no. 1 (Spring 2006): 31-75, quote on p. 34, https://doi.org/10.1177/0003603X0605100103.

[34] O.V. Ustymenko and V.I. Bilyk, "Planuvannja rozvytku spromozhnostej syl oborony Ukrai'ny shhodo protydii' zagrozam u hodi gibrydnoi' vijny [Planning for the Development of the Capabilities of the Ukrainian Defence Forces to Counter the Threats During the Hybrid War]", *Bulletin of the National Academy of Public Administration under the President of Ukraine* 2 (2018): 48-52, http://nbuv.gov.ua/UJRN/vnaddy_2018_2_9.

[35] Hari Bucur-Marcu, Philipp Fluri, and Todor Tagarev, eds., *Defence Management: An Introduction* (Geneva: DCAF, 2009).

[36] Todor Tagarev, "Capabilities-based Planning for Security Sector Transformation," *Information & Security: An International Journal* 24, (2009): 27-35.

[37] Yurii Androsik, "Biznes–jekosistemy kak forma razvitija klasterov [The Business Ecosystems as a Form of Cluster Development]," Belorusskij gosudarstvennyj tehnologicheskij universitet, *Trudy BGTU*, 7, no. 189 (2016): 38-43. https://elib.belstu.by/handle/123456789/20306.

About the Author

Oleksandr M. **Polischuk** holds a Masters degree in Public Administration in the field of National Security. He is graduate of the Royal College of Defence Studies (UK, 2010) and The Netherlands Defence College (The IDL, Rijswijk, 1998). Currently, Oleksandr is a postgraduate student at the National Institute for Strategic Studies in Kyiv, Ukraine. https://orcid.org/0000-0002-4915-8103.